? t 8/5/1,2,4,5,6

8/5/1
DIALOG(R)File 351:DERWENT WPI


012542973 **Image available**
WPI Acc No: 99-349079/199930
XRPX Acc No: N99-261111
*Encrypter* e.g. for public key cryptosystem
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE )
Inventor: OKAMOTO T; UCHIYAMA S
Number of Countries: 027 Number of Patents: 004
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Main IPC | Week |
|---|---|---|---|---|---|---|---|
| EP 924895 | A2 | 19990623 | EP 98123917 | A | 19981216 | H04L-009/30 | 199930 B |
| JP 11174955 | A | 19990702 | JP 97347613 | A | 19971217 | G09C-001/00 | 199937 |
| JP 11231774 | A | 19990827 | JP 9831561 | A | 19980213 | G09C-001/00 | 199945 |
| CA 2256179 | A1 | 19990617 | CA 2256179 | A | 19981216 | H04L-009/30 | 199949 |

Priority Applications (No Type Date): JP 9831561 A 19980213; JP 97347613 A 19971217
Patent Details:

| Patent | Kind | Lan | Pg | Filing Notes | Application | Patent |
|---|---|---|---|---|---|---|
| EP 924895 | A2 | E | 28 | | | |
| Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI | | | | | | |
| JP 11174955 | A | | 13 | | | |
| JP 11231774 | A | | 8 | | | |
| CA 2256179 | A1 | E | | | | |

Abstract (Basic): EP 924895 A2

NOVELTY - The *encrypter* has an exponent generator to generate an exponent by combining an input plaintext m and a *random* *number* r. An exponentiating device *generates* a ciphertext by exponentiating a *second* public *key* g with the exponent in a modular-n reduced residue class group, where the n is a first public key which is a composite number.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a decryption device for a public key cryptosystem, a recording medium on which there is recorded a program for executing an *encryption* process of an *encryption* device through the use of two public keys n and g, a recording medium on which there is recorded a program for executing a decryption process of an *encryption* device through the use of two public keys n and g, a recording medium on which there is recorded a program for executing an *encryption* process of an *encryption* device which uses an elliptic curve over a modular-n residue ring where the n is obtained by the Chinese remainder theorem from a public key, an elliptic curve Ep over a finite field Fp having a number p of Fp -rational points and an elliptic curve Eq over a finite field Fq having a number q of Fq -rational points, and a recording medium on which there is recorded a program for executing a decryption process of a decryption device for decrypting an input ciphertext C, where let p be an odd prime larger than 5, Ep be an elliptic curve over a finite field Fp and having a number p of Fp-rational points, its two Fp-rational points be non infinite points Gp and Cp and lambda (GP)-1 mod p be a